Stream Ciphers Livianos estandarizados mediante normas internacionales para ser usados en Internet de las Cosas

Jorge E. ETEROVIC
Facultad de Ingeniería, Universidad del Salvador - USAL
Ciudad Autónoma de Buenos Aires-C1023AAB, Argentina
y
Marcelo J. CIPRIANO
Facultad de Ingeniería, Universidad del Salvador - USAL
Ciudad Autónoma de Buenos Aires-C1023AAB, Argentina

RESUMEN

El presente trabajo indaga acerca del origen y naturaleza de los algoritmos criptográficos del tipo Stream Ciphers, pertenecientes a la llamada Criptografía Liviana o Ligera y reconocidos por una norma internacional ISO/IEC. Se estudia además el contexto y año de su creación, estandarización, su origen en el ámbito académico o empresarial y se presenta una breve reseña acerca de su funcionamiento y contexto de uso.

Palabras Claves: RFID, WSN, Lightweight Cryptography, Stream Ciphers, ISO/IEC 18033 y ISO/IEC 29192.

1.INTRODUCCIÓN

Los diversos dispositivos del tipo *Internet de las Cosas (*también conocidos por sus siglas en inglés IoT: *Internet of Things*) prometen cambios sociales-culturales y económicos nunca vistos a la fecha. Básicamente estos dispositivos se agrupan en dos clases: *RFID*[1] y *WSN*[2]. Ellos producen, procesan, envían y reciben información que su uso incorrecto o en poder de personas inescrupulosas podría provocar daños. Por ejemplo: es posible para un pirata informático provocar un mal funcionamiento de un dispositivo médico afectando la salud de la persona que lo porta, como son las bombas de insulina o marcapasos inteligentes [1-2].
Los dispositivos *IoT* tienen una característica en común: son aparatos limitados en tamaño, consumo de energía, poder de cómputo, almacenamiento y alcance de la señal. Razón por la cual asegurar los enlaces de comunicaciones desde y hacia estos equipos es una tarea muy difícil: la criptografía tradicional es inaplicable a estos dispositivos pues son incapaces de satisfacer los requerimientos operacionales que esa criptografía precisa.
La llamada *Criptografía Liviana o Ligera* (*Lightweight Cryptography* en inglés) es la respuesta que la comunidad científica ha encontrado para usar en estas reducidas condiciones de cómputo. La norma I*SO/IEC 29192-1* del año 2002 define a este tipo de criptografía.
Este trabajo centra su estudio en los algoritmos de tipo *Cifradores en Cadena* o *Stream Ciphers* que se pueden emplear en dispositivos de tipo RFID. Se listará los algoritmos livianos reconocidos y estandarizados por normas internacionales. El año en que fueron creados, quiénes fueron sus autores. La universidad o empresa que patrocinó su diseño y el contexto en el que nacieron.

2.BENEFICIOS DE LA ESTANDARIZACIÓN

Los primeros algoritmos criptográficos en ser estandarizados y tener una norma internacional fueron del tipo *Cifradores en Bloque* o *Block Ciphers*, a los que con posterioridad les siguieron los *Stream Ciphers*.
Tal es el caso del algoritmo AES (Advanced Encryption Standard) que fue reconocido en el 2005 en la norma *ISO/IEC 18033-3:2005"Information technology. Security techniques. Encryption algorithms. Part 3: Block ciphers"*, junto a los algoritmos TDEA, MISTY1, CAST-128, Camellia, SEED.
Uno de ellos es una variante del *algoritmo DES* (Data Encryption Standard: algoritmo que fue sustituido por el AES) llamado *TDEA*[3]. Y a partir de allí, otros *Block Ciphers* han sido normalizados.
Las ventajas que se obtienen de implementar algoritmos reconocidos en estándares internacionales son, entre otras:

- Libre disponibilidad del algoritmo para su uso.
- Descripción detallada de las funciones que lo conforman, como así también del diseño en general.
- Verificación del funcionamiento y conformidad de un grupo independiente de expertos.
- Existencia de "Test Vectors"[4] para la corroboración del buen funcionamiento de los mismos.

3.CARACTERÍSTICAS DE LOS STREAM CIPHERS

Aunque son reconocidos desde hace mucho, los Stream Ciphers son definidos en la norma *ISO/IEC 18033-1:2015 "Information technology. Security techniques. Encryption algorithms. Part 1: General":* son sistemas de cifrado cuyo algoritmo tenga la propiedad de combinar una secuencia de símbolos de texto plano con una secuencia de símbolos de la clave (o secuencia cifrante), un símbolo a la vez, utilizando una función invertible. Así:

$$E_k(m_i) = c_i \quad (1)$$

$$E_{(k,\,vi)}(m_i) = m_i \oplus k_i \quad (2)$$

$$D_{(k,\,vi)}(c_i) = m_i \quad (3)$$

$$D_{(k,\,vi)}(c_i) = c_i \oplus k_i \quad (4)$$

Siendo $E_{(k,\,vi)}$ la *Función de Cifrado* para la clave *k* y vector de inicialización *vi;* $\oplus$ la función *XOR*; m_i el símbolo *i* del mensaje; k_i el símbolo *i* de la secuencia cifrante y c_i el símbolo *i* del texto cifrado. A su vez $D_{(k,\,vi)}$ es la *Función de Descifrado*.
Un *vi* o *Vector de Inicialización* es una secuencia de bits que se introducen en el algoritmo, junto a la clave. Su finalidad es impedir mensajes iguales sean cifrados idénticamente. Así si un atacante estuviese "mirando" el canal de comunicaciones no advertiría una retransmisión.

4.NORMAS ISO/IEC 18033 Y 29192

La norma *ISO/IEC 18033-4:2011 "Information technology. Security techniques. Encryption algorithms. Part 4: Stream ciphers"* presenta 5 algoritmos de Cifrado de Flujo. Cada uno definido detalladamente, su forma de trabajo, la carga de la clave

[1] Radio Frequency Identificacion: Identificación por Radio Frecuencia.
[2] Wireless Sensors Networks: Redes de Sensores Inalámbricos.
[3] TDEA: Triple Data Encryption Algorithm. Es también conocido por el nombre de Triple DES.
[4] Test Vectors o Vectores de Prueba: dadas ciertos estados iniciales de los algoritmos, se listan los primeros *n* bits de su salida.

k y el vector de inicialización *iv*, entre otra información relevante. La norma *ISO/IEC 29192-1:2012* Information technology. Security techniques. Lightweight Cryptography. Part 1: General" introduce una nueva área de la Criptografía, conocida con el nombre de *Criptografía Liviana o Ligera*, con fines de confidencialidad, autenticación, no repudio e intercambio de claves. Es decir, todo lo que la Criptografía *"tradicional"* permite llevar a cabo.
Este nuevo campo de investigación vio la luz con el advenimiento de los llamados "*entornos restringidos o limitados*", aquellos donde se destacan limitaciones de acuerdo a criterios como:

- *Área del Chip.*
- *Consumo de energía.*
- *Ciclos*
- *Bits por ciclo.*
- *Potencia consumida*
- *Energía por bit*
- *Tamaño del código del programa.*
- *Tamaño de la memoria RAM.*
- Latencia

Partes de esta norma presentan soluciones criptográficas livianas, como por ejemplo *Block Ciphers* (parte 2), mecanismos asimétricos para el *Intercambio de Claves* (parte 4), *Algoritmos de Hash* (parte 5), *Códigos para Autenticar Mensajes* (parte6), entre otras técnicas. Las que serán motivo de otras investigaciones dadas sus importantes aplicaciones.
En especial es de interés para este trabajo la *ISO/IEC 29192-3:2012* "*Information technology. Security techniques. Lightweight cryptography. Part 3: Stream ciphers"*. En ella se presentan dos *Stream Ciphers Livianos*. Ambos están orientados a hardware, esto significa que fueron pensados y optimizados para que sean implementados directamente en ese entorno de trabajo, por sus características y propiedades de diseño.

ISO/IEC 18033	ISO/IEC 29192
Decim-v2	*Enocoro*
KCipher-2 (K2).	
MUGI.	
Rabbit	*Trivium*
SNOW 2.0.	

Tabla 1: algoritmos contenidos en las normas ISO/IEC.

5. ALGORITMOS LIVIANOS

Decim-V2.

Es un algoritmo orientado a Hardware [3]. Fue creado en 2005 por *Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Blandine Debraize, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin* y *Hervé Sibert*. El gobierno, empresas y centros de estudios franceses patrocinaron la creación de este algoritmo a través del *INRIA (Instituto Nacional de Investigación en Informática y Automatización.)*, Axalto Smart Cards, Cryptolog International, France Telecom, Departamento de Informática de la Ecole Normale Superieur y el Laboratoire PriSM de la Universidad de Versailles. *DECIM* fue presentado en el *eSTREAM*[5] [4] (patrocinado por el *E-CRYPT*[6])

[5] eSTREAM: Proyecto de investigación europeo (2004-2008) con el propósito de "Identificar nuevos cifrados de flujo adecuados para una adopción generalizada".

[6] ECRYPT: *European Network of Excellence in Cryptology*. Iniciativa europea con el objetivo de promocionar la colaboración principalmente de investigadores europeos en el campo de la Seguridad de la Información, con énfasis en la Criptología, entre otros.

Avanzó hasta la ronda final del concurso, aunque no fue incluido en el portfolio final, conformado por 3 Stream Ciphers orientados a Hardware (Grain, Mickey y Trivium) y 4 orientados a Software (HC-128, Rabbit, Salsa20/12 y Sosemanuk).
DECIM-V2 es la versión mejorada a la que fue presentada en el concurso. Utiliza 80 bits de clave y 64 bits de vector de inicialización.

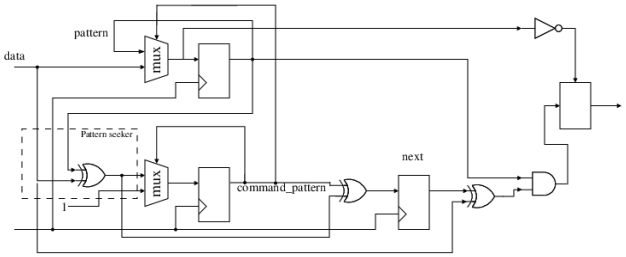

Figura 1: esquema del algoritmo DECIM-V2.

Existe además una versión presentada en 2007, llamada *DECIM-128* trabaja con una clave y un vector de inicialización de 128 bits cada uno.

Enocoro.

Es una familia de Generadores de Números Seudo-aleatorios, creado en 2007 para la empresa japonesa *HITACHI* por *Dai Watanabe, T. Kaneko* [5] que puede usarse como Stream Cipher. Es una variante del algoritmo *Panamá*[7] propuesto en el *5th International Workshop Fast Software Encryption* del año 1998.

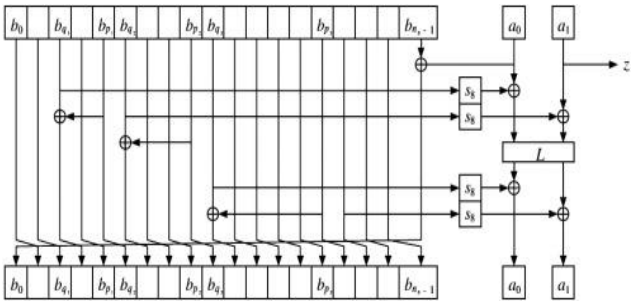

Figura 2: esquema del algoritmo Enocoro.

ENOCORO tiene dos variedades: una de 80 bits y otra de 128 bits conocidas como *ENOCORO-80* y *ENOCORO-128v2* [6]. El proyecto *CRYPTREC*[8] [7] lo incluyó en la lista de "candidatos" del año 2013.

KCipher-2.

También conocido por el nombre K2, es un algoritmo creado por *Shinshaku Kiyomoto, Toshiaki Tanaka* y *Kouichi Sakurai* en conjunto para *KDDI Research Inc*[9] y la *Universidad de Kyushu, Japón*. Fue presentado en el año 2007 en el *3th The State of the Art of Stream Ciphers (SASC-07)* [8].

[7] PANAMA es un algoritmo creado por *Joan Daemen y Craig* Clapp en 1998. Puede ser usado como Stream Cipher y como Hash. Ha manifestado algunas vulnerabilidades como hash. Una de sus variantes que resuelve las debilidades, llamada *RadioGatún* ha inspirado al algorimo *Keccak*, el que recientemente ha sido elegido como el *SHA-3 (Secure Hash Algorithm)*.

[8] CRYPTREC: Comité de Investigación y Evaluación de Criptografía creado por el Gobierno japonés para evaluar y recomendar técnicas criptográficas para uso gubernamental e industrial. Se inició en el año 2000 y la primera "Lista de Algoritmos Recomendados" fue publicada en 2003. La revisión de la misma se publicó en 2013.

[9] KDDI Research Inc: empresa destinada a la investigación, cuyos accionistas son las corporaciones KDDI, KYOCERA y TOYOTA MOTOR.

KCIPHER-2 es un algoritmo orientado a Software y muy veloz dada su sencillez. Puede ser implementado en Hardware por sus propiedades de paralelización.
Sus autores lo ubican en la categoría "*Criptografía Liviana*" dado que mantiene altas prestaciones en entornos reducidos en recursos [9-10].

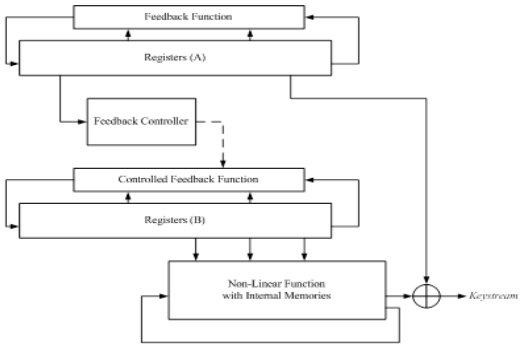

Figura 3: esquema modular del algoritmo KCIPHER-2.

Emplea 128 bits de clave y 128 bits de vector de inicialización.
Hasta el momento no se conocen vulnerabilidades frente a ataques. El proyecto *CRYPTREC* del gobierno japonés lo colocó en la *Lista de Algoritmos Recomendados para el Gobierno Electrónico* [11-12] y recomienda su uso.

Mugi.

Es un algoritmo creado por D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi para la empresa japonesa *HITACHI* en el año 2001.

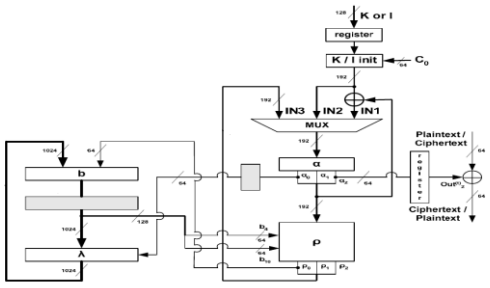

Figura 4: esquema del algoritmo MUGI.

Fue presentado en el *9th International Workshop Fast Software Encryption* del año 2002[12]. Es una variante del algoritmo *Panamá* propuesto en el *5th FSE 1998*. Tiene una clave secreta y un vector de inicialización de 128 bits cada uno. Originalmente orientado a Hardware, también mostró muy buen rendimiento en Software.
El proyecto *CRYPTREC* lo colocó en la lista de *Lista de Algoritmos Recomendados para el Gobierno Electrónico* [13] en el año 2003. Sin embargo, en la revisión de algoritmos del año 2013, *MUGI* cambió de categoría y pasó a la de "candidato". Cabe aclarar que este cambio no fue por haberse detectado debilidades en su seguridad, sino porque esos algoritmos no son de tan amplia difusión como otros.

Rabbit

Este algoritmo fue creado por *Martin Boesgaard*, *Mette Vesterager*, *Thomas Christensen* y *Erik Zenner* pertenecientes a la empresa dinamarquesa *CRYPTICO A/S*.
En su diseño se pueden observar ciertas características de optimización orientado a software.
El algoritmo trabaja con una clave de 128 bits de longitud y un vector de inicialización de 64 bits.
Fue presentado en el año 2003[14] en el *10th International Workshop FSE*[10].

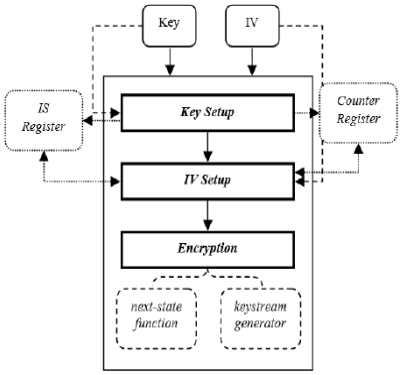

Figura 5: diagrama conceptual del algoritmo RABBIT.

Aunque se conoce un sesgo en los bits de salida de Rabbit, esto no reduce la seguridad del mismo pues la complejidad del ataque es mayor que la del ataque por "Fuerza Bruta".

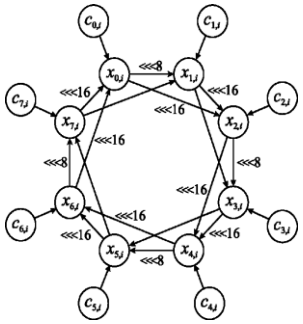

Figura 6: detalle de la función Next-State del algoritmo RABBIT.

En el año 2005 ingresó al *eSTREAM* [15] y es uno de los algoritmos incluidos en el portfolio final. Estuvo bajo tratativas de patentamiento, pero finalmente fue liberado en el año 2008.

Snow 2.0.

Se conoce como *Snow* o *Snow 1.0* a la primera versión de este algoritmo, publicada en 2003[14]. Fue creado por *Thomas Johansson y Patrik Ekdahl* en la *Universidad Lund, Suecia*. Fue presentado originariamente en el *NESSIE*[11] *(New European Schemes for Signatures, Integrity and Encryption)* [16-17].

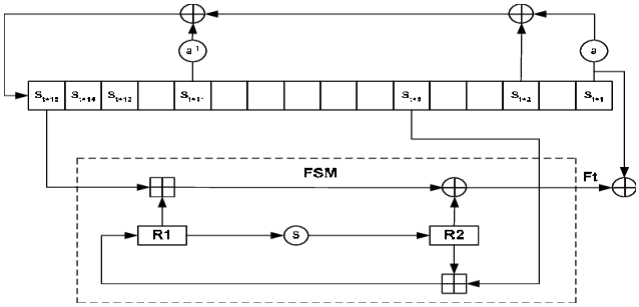

Figura 7: esquema del algoritmo SNOW-2.0

El algoritmo trabaja con palabras de 32 bits y permite usar claves de 128 y 256 bits. Durante el proceso de evaluación de *NESSIE* fue descubierta una vulnerabilidad y retirado de la competencia.

[10] FES: Fast Software Encryption. La edición 10 de este congreso fue organiza en la Universidad Lund, Suecia.
[11] NESSIE: Proyecto de investigación europeo (2000-2003) para la búsqueda de nuevos estándares para Europa de firmas, integridad y cifrado. Es equivalente al concurso del AES patrocinado por NIST (Estados Unidos) y su par japonés, el CRIPTREC.

Por lo que, una vez resuelta, sus autores presentaron la versión mejorada bajo el nombre *SNOW 2.0*.

Trivium.

Este algoritmo fue creado por *Christophe De Cannière y Bart Preneel* de la *Graz University of Technology* en *Austria* y la *Katholieke Universiteit Leuven en Bélgica*.

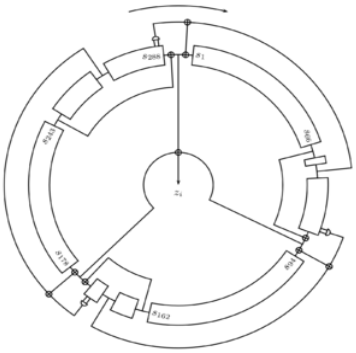

Figura 8: esquema del algoritmo Trivium.

Trivum se presentó en el 2005 en el *eSTREAM* en el área de Hardware [18-19]. Al finalizar este proyecto fue uno de los finalistas e incluido en el portfolio.
Es un algoritmo compuesto por un estado interno de 288 bits, formado por tres registros de desplazamiento. Emplea funciones booleanas no lineales para la obtención del bit de salida y de realimentación, formada por bits de los 3 registros. Tiene una longitud de clave y de vector de inicialización de 80 bits cada uno.
La siguiente tabla presenta de forma sintética la información de los algoritmos Stream Ciphers Livianos bajo normas ISO/IEC, ordenada por año de publicación.

6. CONCLUSIONES

A partir de la lectura y análisis de las normas ISO/IEC 18033e ISO/IEC 29192 de los años 2011 y 2012 respectivamente, se puede vislumbrar el interés internacional para la estandarización de algoritmos de cifrado de tipo Stream Ciphers y los beneficios que de ella se desprenden. Tanto sea para organismos gubernamentales, empresas o usuarios en general.
Esta "*ola de estandarización*" alcanza a los algoritmos pertenecientes al campo de la Criptografía recientemente creado, llamado *Criptografía Ligera o Liviana*. El mismo surge a partir de la necesidad de dotar de confidencialidad, autenticación y demás propiedades a los enlaces de comunicaciones entre dispositivos que deben trabajar en los llamados "*entornos restringidos o limitados*".
Estas limitaciones se manifiestan en la reducida capacidad de cómputo, la búsqueda del mínimo consumo de energía, la disminución del tamaño de los microprocesadores, entre otras. Tal es el caso de los equipos pertenecientes a la llamada "*Internet de las Cosas*" (IoT) y todos los dispositivos por venir, ya que este ahorro o reducción de recursos es la tendencia que se observa en los últimos tiempos.
El gobierno de Japón y la Comunidad Europea encabezan este interés internacional por la normalización. Ellos han patrocinado diferentes concursos para la presentación de nuevos algoritmos y la posterior selección de los mejores.
También se puede observar que la mayoría de ellos surgen en el seno de universidades y laboratorios de investigación del ámbito académico. Unos pocos nacieron en el seno de empresas u organismos mixtos.
La siguiente tabla presenta de forma sintética información acerca de los algoritmos Stream Ciphers Livianos estandarizados bajo normas ISO/IEC.

Año de Publicación	Nombre	Norma ISO/IEC	Autores
2001	Mugi	18033-4 (2011)	Watanabe, Furuya, Yoshida, Takaragi, Preneel.
2003	Rabbit.	18033-4 (2011)	Boesgaard, Vesterager, Christensen, Zenner.
	Snow 2.0.	18033-4 (2011)	Ekdahl, Johansson.
2005	Decim-v2.	18033-4 (2011)	Berbain, Billet, Canteaut, Courtois, Debraize, Gilbert, Goubin, Gouget, Granboulan, Lauradoux, Minier, Pornin, Sibert.
	Trivium	29192-1 (2012)	De Cannière, Preneel.
2007	Enocoro	29192-1 (2012)	Watanabe, Kaneko.
	KCipher-2	18033-4 (2011)	Kiyomoto, Tanaka, Sakurai

Tabla 2: algoritmos Stream Ciphers bajo normas ISO/IEC**.**

7. AGRADECIMIENTOS

Los autores agradecen a la Universidad del Salvador, a su Facultad de Ingeniería, a su personal de gestión, docentes, alumnos y al *Instituto de Investigación en Ciencia y Tecnología* por el apoyo brindado a lo largo del camino recorrido por los proyectos VRID 1737 y VRID 1739.

8. REFERENCIAS

[1] W. Burleson and K. Fu, **Design Challenges for Secure Implantable Medical Devices, Proceedings of the 49th Annual Design Automation Conference,** 2012.
[2] D. Halperin, T. Heydt-Benjamin, B. Ramsford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. Maisel, **Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.** Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008.
[3] O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. **Decim – A new Stream Cipher for Hardware applications**. En ECRYPT Stream Cipher Workshop SKEW 2005.
[4] http://www.ecrypt.eu.org/stream/portfolio_revision1.pdf. (consultada el 12/6/2017).
[5] D. Watanabe and T. Kaneko, **A construction of light weight Panamalike keystream generator.** Information Security and Cryptology: 7th International Conference, Inscrypt 2011. Revised Selected Papers. Springer. Beinjing.
[6] D.Watanabe, K. Okamoto and T. Kaneko, **A Hardware-Oriented Light Weight Pseudorandom Number Generator Enocoro-128v2**. Symposium on Cryptography and Information Security, SCIS2010, 3D1-3, 2010 (in Japanese).
[7] http://www.cryptrec.go.jp/english/images/cryptrec_01en.pdf (consultada el 12/6/2017).
[8] http://www.cryptrec.go.jp/english/cryptrec_03_spec_cypherlist_files/PDF /1002espec.pdf. (consultada el 12/6/2017).
[9] Kiyomoto, S., Tanaka, T., and K. Sakurai, **A Word-Oriented Stream Cipher Using Clock Control,** Proc.SASC 2007, pp. 260-274.
[10] https://www.kddi-research.jp/sites/default/files/products/kcipher2/specification.pdf (consultada el 12/6/2017).
[11] http://www.ecrypt.eu.org/stream/papersdir/2007/029.pdf (consultada el 12/6/2017).
[12] Watanabe D., Furuya S., Yoshida H., Takaragi K., Preneel B. A **New Keystream Generator MUGI**. En Daemen J., Rijmen V. (eds) Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science, vol 2365. Springer, Berlin, Heidelberg.
[13] http://www.cryptrec.go.jp/english/method.html (consultada el 12/6/2017).

[14] Boesgaard, M.; Vesterager, M.; Pedersen, T. Christiansen, J. and Scavenius, O. **Rabbit: A New Hagh-Performance Stream Cipher**. Fast Software Encryption. 10th International Workshop, FSE 2003, LUND, Sweden. 2003.
[15] http://www.ecrypt.eu.org/stream/p3ciphers/rabbit/rabbit_p3.pdf (consultada el 12/6/2017).
[16] Ekdahl, P,; Johansson, T.A **New Version of the Stream Cipher SNOW**. Springer-Verlag Berlin Heidelberg.2003.
[17] https://competitions.cr.yp.to/nessie.html (consultada el 12-6-2017).
[18] Biryukov, A.; De Canniere, C.; et all. **Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption.** Springer-Verlag Berlin. 2004.
[19] http://www.ecrypt.eu.org/stream/papersdir/2006/021.pdf (consultada el 12/6/2017).